UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/714,380	10/31/2003	Stephen M. Trimberger	X-1435 US	1825

24309 7590 09/06/2007

XILINX, INC
ATTN: LEGAL DEPARTMENT
2100 LOGIC DR
SAN JOSE, CA 95124

EXAMINER	
MORAN, RANDAL D	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
09/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/714,380	TRIMBERGER, STEPHEN M.	
	Examiner	Art Unit	
	Randal D. Moran	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 June 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20 and 22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20,22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-20, and 22 are pending in this application.

2. Below, Examiner has pointed out particular references contained in the prior art(s) of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claims, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully each reference in its entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Claim Rejections - 35 USC § 101

1. The rejection under U.S.C. 101 has been overcome by the amendment filed 6/18/2007. However, the addition of "computer program product" and "computer-usable medium" raises a U.S.C. 112 new matter issue.

Claim Rejections - 35 USC § 112

1. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2. **Claims 20 and 21** are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

- Considering **Claim 20**- lines 1-3 and **Claim 22**- line 1, the claim recites new matter in the form of "computer program product" and "computer-usable medium" which has not been previously discloses in the specification.

Specification

1. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: No antecedent basis is provided for "computer program product" and "computer-usable medium" in **Claims 20 and 22**.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. **Claims 1, 4-12, 14, 20-22**, are rejected under 35 U.S.C. 102(b) as being anticipated by **Garnett (US 6,356,637)**.

3. Considering **Claims 1, 9, and 12,** Garnett discloses a system of securely using decryption keys during Programmable Logic Device (PLD) configuration (abstract), comprises: a microcontroller within the PLD for receiving an encrypted bitstream (Fig 1- item 3, item 5, and item 9, column 7- lines column 7- lines 35-41); a key storage register coupled to the microcontroller for storing key data (Fig. 1- item 6, column 5- lines 19-30); a decryptor coupled to the key storage register, wherein only the decryptor can read from the key storage register (Fig. 1, Fig. 4- column 6- lines 50-62); and a configuration data register in the PLD (column 7- lines 14-30, wherein the configuration data register cannot be read by the microcontroller after the decryptor is used (Fig. 1, Fig. 6- item 3 and item 17, column 5- lines 52-60, column 7- lines 5-13 and 35-57).

4. Considering **Claim 4,** Garnett discloses the decryptor is a software decryptor stored in a memory that uses hardware to enable access to the key storage

register based on a memory address (column 4- lines 10-21, column 7- lines 38-49).

5. Considering **Claims 5 and 10,** Garnett discloses the memory is a ROM having a decryption engine (column 2- lines 17-20).

6. Considering **Claims 6 and 11,** Garnett discloses the microcontroller further receives a configuration boot program along with the encrypted bitstream (Fig. 6- item 4, column 4- lines 22-27).

7. Considering **Claim 7,** Garnett discloses the microcontroller, the key register, the decryptor, and the configuration data register are all within the PLD (Fig. 1, Fig. 6).

8. Considering **Claim 8,** Garnett discloses the microcontroller is an emulated microcontroller in the PLD (Fig. 6- item 3 and item 17, column 4- lines 22-27).

9. Considering **Claim 14,** Garnett discloses the configuration data register cannot be read by the microcontroller while the decryptor is used (column 6- lines 55-62).

10. Considering **Claim 16,** Garnett discloses only the decryptor can read from the key storage register (Garnett- Fig. 4).

11. Considering **Claim 20,** Garnett discloses a bitstream, comprising: a configuration boot program for running a microcontroller on a programmable logic device; and an encrypted bitstream portion of the bitstream containing encrypted configuration data for a configuration data register on the programmable logic device (Fig. 1- item 4 and item 9, column 4- lines 22-27).

12. Considering **Claim 22,** Garnett discloses said configuration boot program comprises instructions for a decompressor (Fig. 1- item 3 and item 5).

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. **Claims 2, 3, 13, and 15-18** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Garnett** in view of **Pang et al. (US 6,366,117),** hereafter "Pang."

3. Considering **Claim 2 and 13,** Garnett does not disclose the microcontroller stores key data in the key storage register, but the microcontroller cannot read from the key storage register.

Pang does disclose the microcontroller stores key data in the key storage register, but the microcontroller cannot read from the key storage register (Fig. 3- item 26 and item 29, column 16- lines 8-40).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Garnett by not allowing the microcontroller to read from the key storage register as taught by Pang in order to provide enhanced security against the loss of commercially valuable intellectual property (Garnett- abstract). Unless the design were re-encrypted for the read-back operation, the act of reading back the bitstream would expose the unencrypted bitstream to view. Further security of the design is provided by disabling readback when an encrypted design is loaded into the FPGA (Pang- column 19- lines 63-67, column 20- lines 1-4).

4. Considering **Claim 3,** the combination of Garnett and Pang discloses the decryptor is a hardware decryptor embedded in an integrated circuit along with the PLD (Garnett- column 2- lines 11-16, column 4- lines 10-21).

5. Considering **Claim 15,** the combination of Garnett and Pang discloses the microcontroller cannot read from the key register (Pang- Fig. 3- item 26).

6. Considering **Claim 17,** the combination of Garnett and Pang discloses the steps of loading the decryptor with data from key register and loading the decryptor with data from the microcontroller comprises using a predetermined instruction enabling access to the key storage register based on a known address of a memory storing a decryption engine forming the decryptor (Garnett- Fig. 4, column 4- lines 10-21, column 6- lines 53-55, column 7- lines 42-57, Pang- column 5- lines 44-61).

7. Considering **Claim 18,** the combination of Garnett and Pang discloses a system of securely using decryption keys during programmable logic device configuration (Garnett- abstract), comprises: a memory-mapped key register coupled to a microcontroller data bus (Garnett- Fig. 6- item 3 and item 6); a decryptor engine stored in non-volatile memory and coupled to the microcontroller data bus (Garnett- Fig. 4); logic circuitry limiting access to the key register from the microcontroller data bus using specified addresses of the non-volatile memory (Pang- Fig. 3- item 28, column 5- lines 44-61, column 15- lines 49-61).

1. **Claim 19 is** rejected under 35 U.S.C. 103(a) as being unpatentable over **Garnett** and **Pang** in view of **Kuranaga (US 5,409,661).**

2. Considering **Claim 19,** the combination of Garnett and Pang does not disclose the logic circuitry uses specified addresses of the non-volatile memory by limiting

access to minimum and maximum ROM memory addresses using a microcontroller program counter.

Kuranaga does disclose the logic circuitry uses specified addresses of the non-volatile memory by limiting access to minimum and maximum ROM memory addresses using a microcontroller program counter (column 6- lines 56-67).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Garnett and Pang by logic circuitry that uses specified addresses of the non-volatile memory by limiting access to minimum and maximum ROM memory addresses using a microcontroller program counter as taught by Kuranaga in order to provide enhanced security against the loss of commercially valuable intellectual property (Garnett- abstract).

Response to Arguments

1. Applicant's arguments filed 6/18/2007 have been fully considered but they are not persuasive.

2. Regarding **Claims 1, 9, and 12,** applicants arguments have been fully considered but they are not persuasive. With respect to applicants argument that Garnett fails to teach "a microcontroller within the PLD for receiving an encrypted

bitstream." Examiner disagrees and directs applicant to Garnett – Fig. 1- items 1, 3, 5, and 9, column 7- lines 35-41. A microcontroller is defined as a special-purpose, single chip computer designed and built to handle a particular, narrowly defined task per the "Microsoft Computer Dictionary, 5th Edition".

Garnett discloses:

> "configuration data decryption circuitry, in the form of logic 5 and memory 6, for applying a decryption process to configuration data received through a communication link 10..."

Garnett further discloses:

> "the holding register set 19 also has an input for receiving a trigger signal from the state machine through the state machine communication link 25. Furthermore, the configuration register set 18 has an input for receiving a global reset signal and is designed so that on receipt of a reset signal through this input it adopts a default state."

The ability to receive a global reset signal as well as change states from decryption to operational and back to a default state requires that there be some type of microcontroller within the FPGA. Therefore, Garnett meets the definition of containing a microcontroller as defined above and as described in the claim.

With respect to applicants argument that Garnett fails to disclose that the "configuration data register cannot be read by the microcontroller after the decryptor is used." Examiner disagrees and directs the applicant to Garnett- Fig. 1, Fig. 6- item 3 and item 17, column 5- lines 52-60, column 7- lines 5-13 and 35-57.

Garnett discloses "the decryption algorithm logic 5 is stateful to further enhance security." Therefore, after the decryptor is used, the configurable logic block changes

state and the FPGA enters an operational mode. Once in operational mode, the configuration data register can no longer be read by the microcontroller.

3. Regarding **Claim 4,** applicants arguments have been fully considered but they are not persuasive. With respect to applicants argument that Garnett fails to teach a "decryptor is a software decryptor stored in a memory that uses hardware to enable access to the key storage register based on a memory address." Examiner disagrees and directs applicant to Garnett- (column 4- lines 10-21, column 6- lines 50-53, column 7- lines 38-49). Garnett discloses "the decryption algorithm embedded in the FPGA." "The encrypted configuration data is input into the FPGA in step 40 and then decrypted in step 41 by applying a decryption algorithm 43." Applying a decryption algorithm (i.e. software decryptor) based on a key stored in key storage (i.e. based on an address) reads on the claim.

4. Regarding **Claims 6, 11, and 20,** applicants arguments have been fully considered but they are not persuasive. With respect to applicants argument that Garnett fails to teach "the microcontroller further receives a configuration boot program along with the encrypted bitstream." Examiner disagrees and directs applicant to Garnett- column 4- lines 22-27. Garnett discloses that "configuration data is transmitted to the FPGA during power-up." Since the on-board memory is used specifically to store keys, it is inherent that the configuration data passed to the FPGA during startup would include boot data. A boot program is necessary in a chip that includes state changes as

well as global resets, all of which come from within the chip and not from external sources.

5. Regarding **Claim 2,** applicants arguments have been fully considered but they are not persuasive. With respect to applicants argument that the combination fails to teach "the microcontroller stores key data in the storage register, but the microcontroller cannot read from the key storage register." Examiner disagrees and directs the applicant to Pang- (Fig. 3- item 26 and item 29, column 16- lines 8-40).

Pang discloses:

> "If key memory 23 is operating in non-secure mode, the 64-bit words can be read from key registers 23b to JTAG bus 25 where the values can be examined external to the FPGA. The FPGA can be tested in this non-secure mode by using 56 bits of a selected 64-bit word in registers 23b as the 56-bit key for DES decryption. In one embodiment, when key memory 23 is in non-secure mode, readback of a user's design is possible even though the design has been encrypted before loading. This allows the designer to test and debug even an encrypted design. Communication of the key security status is through bus 26 (see also FIG. 3).
>
> After values have been written into key registers 23b and verified with a read operation from bus 25, control logic 23a is placed into secure mode by using the ISC_PROGRAM_SECURITY instruction and applying logic 0 to bit 0 of the 64-bit key data bus which is part of the IEEE 1532 standard. In the secure mode, no access to the keys is granted.
>
> As shown in FIG. 11, to assure that an attacker can not return to the nonsecure mode by using the ISC_PROGRAM_SECURITY instruction and then reading out the keys, if the security is eliminated (if the ISC_PROGRAM_SECURITY signal moves to the non-secure logic level), a state machine in control logic 23a erases all keys by writing zeros to all six words, one word at a time. This is done by: in step 110 putting zeros on the wdata[63:0] bus and at step 111 asserting the ws b[0] signal (with a logic 0 value), then at steps 112-117 successively strobing the ws b[0:0] through ws b[5:0] signals one at a time before changing the security status at step 118 and entering the non-secure mode, and finally at step 119 releasing the wdata[63:0] logic 0 values. Thus, any attempt to place battery backed up memory 23 into a non-secure mode causes all values in key registers 23b to be erased."

Once values have been read into the key registers and verified (i.e. microcontroller stores key data), the control logic is placed into a secure mode in which no access to the keys is granted (i.e. microcontroller cannot read).

6. Regarding **Claim 17,** applicants arguments have been fully considered but they are not persuasive. With respect to applicants argument that the combination fails to teach "loading the decryptor with data from the key register and loading the decryptor with data from the microcontroller comprises using a predetermined instruction enabling access to the key storage register based on a known address of a memory storing a decryption engine forming the decryptor". Examiner disagrees and directs the applicant to Garnett- Fig. 4, column 4- lines 10-21, column 6- lines 53-55, column 7- lines 42-57, Pang- column 5- lines 44-61, column 7- lines 49-66.

Garnett discloses:

> "The decryption algorithm uses a decryption key stored in the decryption key storage of the FPGA." "The contents of the configuration register set 18 in the default state, when loaded into the CLB 27, causes the FPGA to operate as a decryption engine..."

Pang discloses:

> "Several of the words, usually at or near the beginning of the bitstream, are used for setting up the configuration process and include, for example, length of a configuration memory frame, and starting address for the configuration data. Bus 19 allows communication between configuration logic 14 and JTAG logic block 13 so that the JTAG port can be used as another configuration access port. Bus 18 allows communication between configuration logic block 14 and configuration memory 12. In particular, it carries addresses to select configuration frames in memory 12, control signals to perform write and read operations, and data for loading into configuration memory 12 or reading back from configuration memory 12."

> "Before key memory 23 can be accessed through JTAG bus 25, the security status (bus 26) is placed in non-secure mode, which can be done using the ISC_PROGRAM_SECURITY instruction (see FIG. 10a) and applying logic 1 to bit 0 of the key data bus. Key memory 23 is written to and read (for verification) from JTAG bus 25 using the ISC_PROGRAM and ISC_READ instructions of the IEEE 1532 standard. Control logic 23a includes a decoder for decoding the 3-bit address signal ADDR from JTAG bus 25 to produce a lowgoing pulse on the addressed one of write strobe lines ws_b[5:0] if the ISC_PROGRAM instruction appears on JTAG bus 25, or a high signal on the addressed one of read select lines rsel[5:0] if the ISC_READ instruction appears on JTAG bus 25. One of the six 64-bit words can be read by applying a high signal to one of the six read select lines rsel[5:0], which causes read multiplexer 23d to place the selected word on the 64 output lines q[63:0]."

The configuration register set is loaded into the CLB to cause the FPGA to operate in its decryption state (i.e. loading the decryptor with data from the key register). Placing the FPGA in a default state (i.e. data from the microcontroller) based on a reset signal or start up reads on a predetermined instruction. Receiving length of a configuration memory frame, and starting address for the configuration data and checking the FPGA status of secure mode allows access to keys based on a 3 bit address signal reads on "enabling access to a key storage register based on a known address."

7. Regarding **Claim 18,** applicants arguments have been fully considered but they are not persuasive. With respect to applicants argument that the combination fails to teach "logic circuitry limiting access to the key register from the microcontroller data bus using specified addresses of non-volatile memory." Examiner disagrees and directs applicant to Pang- column 5- lines 44-61, column 15- lines 49-61). Addresses being specified to read out from the key memory (i.e. specified addresses) coupled with a

secure mode to not allow the microcontroller (i.e. limiting access) to read from the key registry reads on the claim.

8. Regarding **Claim 19,** applicants arguments have been fully considered but they are not persuasive. With respect to applicants argument that the combination fails to teach "the logic circuitry uses specified addresses of the non-volatile memory by limiting access to minimum and maximum ROM memory addresses using a microcontroller program counter." Examiner disagrees and directs the applicant to Kuranga- column 6-lines 56-67. Karanga discloses that based on a Program Counter used to determine the next instruction, values are loaded from a register which correspond to a min and max values of the virtual addresses which directly correspond to the real address located in RAM. This equates to limiting access to max and min addresses based on a program counter.

Conclusion

1. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

2. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Randal D. Moran whose telephone number is 571-270-1255. The examiner can normally be reached on M-F: 7:00 - 4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Randal D. Moran
/RDM/

KIM VU
SUPERVISORY PATENT EXAM.
TECHNOLOGY CENTER 21C